SECURITY NOW!

Transcript of Episode #28

Listener Feedback Q&A #4

Description: Leo and Steve discuss questions asked by listeners of their previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world "application notes" for any of the security technologies they have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-028.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-028-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 28 for Thursday, February 23, 2006, our Listener Questions and Answers No. 4. Steve Gibson, hello.

Steve Gibson: Hey, Leo. Good to be with you face to face again.

Leo: Had a lovely lunch in the beautiful Rogers Cafeteria. And you had your traditional dual ham sandwiches.

Steve: My meal for the day.

Leo: You're preparing for a big Security Now!. Now, we decided every fourth episode, unless there's some burning issue, to answer questions.

Steve: Right.

Leo: And that's great because we get a lot of them.

Steve: Our Mod 4 episode.

Leo: Mod 4, yeah.

Steve: Yeah, there were a few issues that we - couple things from last week that I want to deal with. Actually, from the last Q&A, a couple people - more than a couple, actually, many people thought that I had sort of sidestepped one of the questions we answered four weeks ago about which is the most secure operating system. I sort of summed it up, I guess, and I think I can understood where they would feel that I had sort of wimped out on it. I said, well, Windows is getting better...

Leo: Yeah.

Steve: ...was sort of the way I...

Leo: That was accurate.

Steve: You know, it certainly is accurate. One of the things that - I did a little bit of research because I was sort of curious. And in fact the U.S. CERT, the United States Computer Emergency Readiness Team, they published a rather controversial report recently that showed that, in 2005, Windows and Windows apps had 812 security flaws, whereas UNIX/Linux and its packages had 2,328, like almost three times more. One of the problems is that in the last, I guess it's, what, three years, Linux code has gone from two million lines to six million lines. And we all know that change is the enemy of security. Whenever you're cranking out lots of new code, there's a chance for some problem.

Leo: Well, I'm going to save you a lot more email, Steve, because there's another issue, which is that Microsoft is relied upon for releasing its security flaws, but the Linux community is a much larger community with a lot more people working on the code because it's open source. So you'd expect to see many more flaws discovered. Furthermore, it's not merely those eight million lines of code that's in Linux. There are thousands of other programs that are part of most Linux distributions that are often included in those security bulletins, as well.

Steve: And certainly were included in this case, so you're right. So it's a problem of apples and oranges comparison.

Leo: I think - and people often do this with Firefox and Explorer, too - I think counting the number of exploits is not a way of discovering whether one is more secure than the other.

Steve: Right.

Leo: In fact, you could make a very good case that that would mean Linux is more secure because the exploits have been discovered and patched.

Steve: Of course. Of course.

Leo: You know, maybe there are fewer holes.

Steve: So it's 2,328 fewer vulnerabilities now than there were before.

Leo: And isn't that what you're looking at, is how many vulnerabilities still exist, not how many have been discovered?

Steve: Yeah. The point I wanted to make, basically to sort of get some conclusion to this question, I mean, is to say that security is a process more than it is a product. I think it's the case that the Mac OS, because of its long-term networking heritage coming from UNIX, is, all things considered, more secure as a platform, as a user-friendly commercial platform, than Windows or any of the open source solutions. So, you know, if someone wants a simple result, I would say the Mac OS is going to give the average user much more security than Windows. Which is not...

Leo: But I wouldn't say that the Mac is the most secure version of UNIX, either. I mean, there are far more secure versions of UNIX out there.

Steve: That are tightly bolted down.

Leo: Intentionally made secure. And in fact there is some evidence that Apple has not maybe patched as many of the older programs as they should have. They haven't kept up, in fact, with the code base. But I agree with you, if you're looking for a consumer operating system, it's probably the - I mean, you're not going to use, you know, SecureBSD as your consumer operating system.

Steve: Right. Also, it's certainly the case, too, that it's possible for a user to run Windows in a very secure way, or run UNIX, Linux, or Mac in an insecure way. So again, it's not just the OS or the applications you're using, but it's what you do with it and how you manage your system. You know, are you opening every attachment that you receive in email? That'll get you on a Mac as easily as it will - well, not quite as easily as it will...

Leo: Actually, it won't because there aren't any exploits. And that's part of the issue, too, is how many exploits are there out there. And there are certainly far more.

Steve: The target of opportunity.

Leo: Right.

Steve: Yup.

Leo: So I think that's why I didn't call you on it last time is I didn't feel like you were fudging, I feel like there was no really correct answer. And you said the right thing, which is Windows is getting better.

Steve: Exactly.

Leo: So for those of us who want you to say Mac, we just have to live with it.

Steve: You know, we just want to have red, green, or blue.

Leo: Yeah.

Steve: The other comment from last week's episode, where we talked about how LAN technology works, I talked about DHCP, Dynamic Host Configuration Protocol, that assigns IPs automatically. And we briefly discussed that versus static IPs. A number of people chimed in with very good instances where static IP assignment was valuable - certainly, for example, if you've got network printers, where different machines need to know what IP address the printer's going to have. You can't have it getting its IP automatically if that would mean that it would have its IP floating around.

Leo: Right.

Steve: And the other, the very good example, is if you've got your consumer router doing port forwarding, it's going to be forwarding ports to an IP. So again, you want to make sure that your computer is there at that IP. The cool thing is, you can have DHCP and static IPs coexisting with no trouble at all. So normally in your router config it'll show, like, first IP that's available for it to assign and last IP, or sometimes it's first IP and how many it can assign. So that creates a block which is normally smaller than the size of the subnet. So, for example, if you had - and we talked about the subnet mask thing, also. If you had a subnet mask, which most routers do, of 255.255.255.0, it means you've got 253 available IPs. Most routers will only assign 100, typically, out of that range, giving you plenty of room to give machines and printers a fixed IP that you don't have to worry about floating around.

Leo: I think some of this is just that some of these technologies just haven't caught up with the DHCP world. I mean, eventually you should have zero config so you don't need to know what printer IP address you have. The port forwarding should be kind of more automatic so you don't have to assign a...

Steve: And the printers will be discoverable by the machines on the network, no matter what their IP is.

Leo: Exactly. They just haven't caught up with it yet.

Steve: Right.

Leo: The automated world we live in. Shall we get to the questions?

Steve: Let's do it.

Leo: David from the United Kingdom has one for you. And actually, as we pointed out before, that often these represent many people who've asked the same question. We're just picking on David.

Steve: Right. And in fact, when I'm going through them, I'll see one that keeps coming up. And it's like, okay, a bunch of people have, you know, it's like, this is something I want to address.

Leo: Want to answer that, yup.

Steve: Exactly.

Leo: My question is about what ShieldsUP! shows me when I'm using HotSpotVPN. Normally my home PC appears totally stealthy. That's good. All green lights.

Steve: Yup.

Leo: However, when I use HotSpotVPN, ShieldsUP! shows the SSH, DNS, and HTTPS ports open. Are these ports from my machine or from HotSpotVPN? Is the VPN tunneling ports through my firewall and opening up my PC to attack? What's the deal?

Steve: Great question. The one thing that I would ask anybody to first look at when they're checking things out with ShieldsUP! is what IP are we showing? Because at the top of any ShieldsUP! page I post the IP, which is the IP that our servers are actually probing. So when you're using HotSpotVPN, we will certainly be probing, not the IP of your machine, but the public IP through which HotSpot emerges onto the Internet. Any of the machines behind and that are using HotSpotVPN will have a 10. IP range. The HotSpot guy allocates IPs for all of their clients in the 10. range. So it's 10.something.something.something. I tend to get, like, 10.250.0.22 whenever I'm using HotSpotVPN. So because that's a private IP, no one outside is able to probe that. There isn't a way for me to access any sort of private 10. IP address.

Now, it is the case that a VPN tunnel could tunnel everything through to the machine. But in this case the HotSpot guy is running a NAT system. And so it's Network Address Translation, which is translating the public IP into the 10. IP. So the bottom line is, all we're able to test, and all any hacker is able to see, is the machine run by HotSpot where the private addresses emerge onto the Internet. So it's definitely not your machine. And you've got all the protection of any NAT router.

Leo: In fact, you might even have more because you're using VPN, as well.

Steve: Yes.

Leo: I think this is related. Chad writes from his Yahoo! account: I tried your suggestion of using the Tor Onion Router network - that's an anonymizer - to anonymize my connection for free. But when I run the ShieldsUP! port scanner, it shows I have several ports open, and the rest show as closed. Nothing is stealth. I'm behind a NAT router. I should be all stealth. What's going on?

Steve: Right, now, you're right. This is sort of a related question. And again, we've seen a lot of this. The Tor system is an interesting anonymizing system that we've talked about where you make a connection to a so-called "Onion Router." And Tor is an acronym for The Onion Router. It then makes a connection to another one, which makes a connection to another one. And they deliberately don't keep any logs of who they've connected to, so that after a few hops you emerge on the Internet from that final router. Once again, if you look at the IP that

ShieldsUP! is testing, it'll be the IP of that last router because that's where we're seeing your connection to GRC coming from, so that's what I test. So again, it's not your machine at all. In this case it's not a VPN. It's just sort of a chain link of routers, and we're only seeing the final emergence at the last router.

Leo: So, gang, stop using VPNs and Tor routers when you want to run ShieldsUP!. You're not testing your system.

Steve: That's a very good point. ShieldsUP! will only be testing the status of the machine that you're entering the Internet from, which in these cases is never your own machine.

Leo: It's an interesting exercise, but it's nothing useful, the result. Jan asks: According to AuditMyPC - which is one of these websites you go to where they scare you - these people are able to acquire the private IP address via JavaScript. Shocking. Is this true? I ran an IP check on my machine and found out that the internal IP they showed me was correct. If it is true, and not some sort of trick, it's a little disconcerting. Any suggestions on how to prevent such an acquisition?

Steve: I'm glad you said "the site that tries to scare you" because, I mean, obviously you know about AuditMyPC. I get this question so much.

Leo: They're in the business of selling you security. So they're trying to raise your fear factor a little bit.

Steve: Well, they really are succeeding, unfortunately.

Leo: And in this case they're really kind of fudging it because...

Steve: Well, okay, yes. First of all, what's happening, to answer Jan's question, is that JavaScript is running on her browser, and that JavaScript, which is basically scripting code written by and downloaded by AuditMyPC, is running in her browser and reporting back to them information from inside her network. You know, the other famous instance of this is where you go to a website, and they show you the contents of your hard drive.

Leo: Right.

Steve: It's because your browser that's on your computer...

Leo: It knows.

Steve: ...is showing you your hard drive.

Leo: Not them.

Steve: They can't see it. Exactly. So, you know, it's one of these things that...

Leo: It's a client-side program. Which means it has client-side information. So that means AuditMyPC doesn't know your IP, your internal IP address?

Steve: Well, no. It means they do. But that's the second part of this question. Jan has nothing to worry about with them knowing her IP is 192.168.0.1. About a million people have that IP because that's a private IP given to her by her router. So anyone can and does see the public IP. For example, that's what ShieldsUP! tests when you go to ShieldsUP!.

Leo: Hey, if you go to any website, it knows your IP address.

Steve: They have to because that's the way they get the traffic back to you, back routed across the Internet, back to your location. But all of this stuff that shows you the contents of your hard drive or that says, oh, we know what your private IP is, well, I mean, the fact that you have a private IP means that you're secure because you're behind a router. So that information does them no good, nor does it do anyone with malicious intent any good.

Leo: Although I have to say it does seem like a flaw in JavaScript that it can discover that kind of information.

Steve: Yeah.

Leo: I don't think it should be - there's no - I don't think there's any compelling reason why it should be...

Steve: The whole client-side scripting thing, of course, is a double-edged sword because that gives you lots of functionality, but, boy, at a security cost.

Leo: Maxwell, whom you call an "avid listener" - what, he listens twice?

Steve: Avidly. We have people who write to us and say they listen two or three times to some of our more, you know, dense propellerhead ones.

Leo: Sometimes you have to. He says: I want to securely share files within my own home. I have a cable modem and a router with a wired PC and a wireless laptop. How can I safely and securely use Windows filesharing? He's worried that, if he turns filesharing on - and we used to say this all the time, oh, don't turn on filesharing, it's insecure, and you're in trouble. Is that still a problem?

Steve: The wisdom has changed because NAT routers happened. Consumer routers protect you from things going on within your local area network and provide really good security so long as you remember to turn off, if you don't need it, the Universal Plug and Play feature, which we've mentioned many times does represent a security problem. So the concern about Windows filesharing being used pervasively in a home isn't something that anyone needs to worry about.

Leo: It's inside the router.

Steve: Except he also has wireless. And so the addition of wireless means that he needs to go back to our earlier episodes talking about WPA and WEP encryption, basically how to make your wireless system safe. If he uses that technology, if he makes sure that he's using WPA encryption with a really long password, he's safe, and he can use Windows filesharing with no concern at all.

Leo: Which makes me think now, when we were talking about static IP addresses, if you turn off the DHCP in your router, are you no longer protected by NAT if you're using static IP addresses?

Steve: No. You still have NAT. The only real difference with no DHCP is that you'll have to manually assign IPs to all of your equipment.

Leo: But it doesn't turn the router into a hub. It's still routing, it's still...

Steve: Right, because those IPs are still private. They're still 192.168, and so you'd have to have that whole public/private translation going on.

Leo: So as long as you have a router, you don't have to worry about filesharing. Now, if you weren't on a router, if you were just on a hub or somehow otherwise getting on the Internet with all your systems, that could be a potential problem.

Steve: Yes. The router is the thing that protects you from having a concern with Windows filesharing because it gives you private IP addresses.

Leo: Dean in Cochrane, Alberta, Canada, says: My question is with regards to Hamachi and UDP. Hamachi, you may remember, is that great VPN solution that we mentioned...

Steve: The peer-to-peer VPN.

Leo: That allows you essentially to set up a LAN, a local area network with people anywhere on the Internet.

Steve: Right.

Leo: My understanding is that UDP, which is the protocol that Hamachi uses, is less reliable than TCP. And you mentioned that TCP is preferred for consistent connections. Is it true that Hamachi uses UDP; and, if so, is it smart enough to handle dropped packets properly? Does OpenVPN use TCP or UDP?

Steve: Okay. Good question, actually.

Leo: We did talk about this.

Steve: Well, we did, but this is sort of an interesting flavor of that. The idea is, first of all, to answer the last question first, OpenVPN can run either. And UDP is a preferred technology for any kind of VPN because it allows you to tunnel any protocol, that is, TCP or UDP, in a good way over UDP. Hamachi, because it was written by a guy who really does, you know, Alex Pankratov really does understand this stuff, it uses UDP. It's able to use it well because, if you have a TCP connection which needs reliability, when TCP says, hey, I dropped a packet, send me another one, well, it's able to issue that request within a UDP packet. You can't issue the request within a TCP packet because TCP gives you connections instead of packets. What you really want are packets. So Hamachi is doing the best possible thing, which is to use UDP. And OpenVPN's preferred means of operating is also to use UDP. So everybody's got it covered.

Leo: The point is, I guess, don't confuse the tunnel...

Steve: Right.

Leo: ...with the traffic in the tunnel.

Steve: Right.

Leo: So you build a tunnel. Let's say it's the Channel Tunnel, the Chunnel. You build the tunnel...

Steve: The carrier.

Leo: ...the carrier with UDP because that's the right protocol. But it doesn't mean you can't have reliable connections inside it. That can still be TCP and all of the issues along with it.

Steve: Exactly.

Leo: Benefits along with it. Burt Lasarge of Redford, Michigan asks: The recent revelation of security issues with Google's Search Across Computers desktop search feature - we haven't really talked about that, we should address that - leads me to wonder whether the built-in Windows directory and file encryption security is a sound way of keeping private files private. Would this solve that problem of having my personal files copied to other computers?

Let's just mention that this new feature that was built into the Google desktop search allows you to search, not only your local computer, but other computers. And in order for Google to be able to do that, it has to store the contents, effectively the index of what's in your computers, on its own servers.

Steve: Right.

Leo: Which is...

Steve: Has caused huge security concerns. And privacy concerns.

Leo: And Electronic Frontier Foundation is pointing out that perhaps a police warrant would allow them to then go to Google and say, give us the contents of this fellow's computer, and they'd have it because you'd turned on this Search Across Computers feature. So the EFF, anyway, is recommending that you turn that off. Do you agree?

Steve: No, I absolutely agree. And it's unfortunate, sometimes Google's got great ideas, but they seem to go a little too far.

Leo: I think they just didn't think about what it meant. You know, they know they're trustworthy.

Steve: Remember when they were caching?

Leo: Yes.

Steve: Remember the...

Leo: Same thing. And it didn't work.

Steve: They were going to speed up everyone's connection...

Leo: Terrible idea.

Steve: ...by caching the Internet for you.

Leo: Right.

Steve: And it would cause all kinds of problems.

Leo: Well, because people's passwords were being cached.

Steve: Yeah. You would end up seeing other people's pages by mistake. Oops.

Leo: So Google turned that off in about a day. They still do that Search Across Computers.

Steve: In response to Burt's question, Windows protection, file or folder or whatever kind of encryption, would not help him.

Leo: Because it's unencrypted when you log in.

Steve: Exactly. Basically it's storing it encrypted. But any view of it that the computer or the user or the network sees, it sees it after it's been decrypted on its way out of the file or out of the drive or directory.

Leo: So if Google can search it, it can see it.

Steve: Right.

Leo: So you should worry about that. Now, if you had another program like TruSecure, which we've talked about, encrypting it, if you left it encrypted, you'd be safe. But the minute you unlocked it, same problem.

Steve: Exactly, exactly.

Leo: Another listener asks: I recently purchased a piece of software called FolderLock - does something of the same thing - in an attempt to secure my portable USB device. But I've already been able to bypass the security measures it implements. Hmm. Hmm.

Steve: Yeah.

Leo: Are there any good portable security programs for USB drives?

Steve: Well, we're going to do an entire episode on TrueCrypt because it's a fantastic solution for this. It's open source and free, and they've really just - they've nailed the solution. So let's just say for now, not to preempt ourselves, take a look at TrueCrypt. Anybody who's interested in encrypting folders, files, USB drives, it handles that stuff and does a beautiful job. It's going to be what we end up recommending.

Leo: Yeah, it's really remarkable. George Walker in Tulsa, Oklahoma is interested in general security and the working of the worldwide web and email system. Well, I hope you listened to our last two episodes because we talked a lot about the Internet. What happens once the data leaves my personal network? For example, how secure and private is my data when it's sent over the Internet and through my Internet service provider? What does my ISP know and see about my usage? Can my ISP see my emails? Having an encrypted wireless home network is great, but isn't it pointless once it gets to my ISP and beyond, when anyone can see the data? That's a great question.

Steve: And unfortunately, the answer is yes.

Leo: Yeah. That's why they called WEP "Wired Equivalent Privacy." They didn't say it's private, they said it's the same privacy as wired.

Steve: Right, yeah.

Leo: Which is not very.

Steve: The idea with the issues we've discussed, like locking down a wireless network or using a VPN when you're in a hotspot or in a hotel, we're trying to secure the high risk, the highest risk zone, and keep somebody from being able to exploit that. But it's absolutely true that, even if you have an encrypted wireless network at home, when it leaves your wireless router, the router is decrypting it to send it out to your ISP. So your email is in the clear. And of course this has been a great concern recently with, you know, all the U.S./NSA spying. And there have been, you know, subpoenas issued to grab people's email. ISPs have unencrypted email on their email servers. That's the way the Internet works. By default, email is not encrypted. Just like web pages are stored in web caches, by default, unencrypted. So, I mean, it is the case that the use of the Internet's standard protocols is not encrypted and is only secure as those people who you are trusting to tend it. And if you did have an ISP that was really misbehaving, they could be spying on their own users.

Leo: Well, not even just an ISP, but it also has to hop from server to server to get out to where it's going. And anybody on that server who was untrustworthy could also snoop; right?

Steve: Right.

Leo: It's like sending a postcard. You trust the mailman's not reading it. And the volume of mail is such that probably he's not. But there's always that risk.

Steve: And you put more sensitive stuff...

Leo: In an envelope.

Steve: Exactly, in an envelope, not on a postcard.

Leo: That's why I use PGP. Now, I also use FastMail, which is an independent email company. And I use SSL to FastMail. So my ISP can't see my mail. But FastMail can see my mail.

Steve: Right. Right.

Leo: Somebody's got to store that stuff.

Steve: Ultimately, because email was never really defined as an encrypted technology, sooner or later it's going to be decrypted in order to go public.

Leo: Has to. Unless you use PGP Point-to-Point, and then only your recipient can read it.

Steve: Right.

Leo: Karen Wilson of Murrieta, Georgia, asks: With a VPN, what happens to the initial - Virtual Private Network - what happens to the initial connection I make with my wireless card at a hotel once I've established a VPN? I have sharing of folders turned on when I'm at work and hardwired into my work's LAN. Are they visible to others in the hotel when I'm using the VPN?

Steve: Correct, a great question. The answer is she is safe. The initial connection establishes the tunnel, and no - and this is really important. This is just like with SSL, where you are creating a secure connection to a remote web server. That connection creates a tunnel. It is brought up and encryption is activated before any user application data first moves through it. So she could be totally comfortable using a VPN in a hotel to connect into her work computer or work network, even though it's got Windows filesharing enabled. There's no leakage through the VPN.

Leo: Now, when I first log into my hotel's network, wireless network, I have to give it a password. I mean, that's kind of part of the deal with a hotel.

Steve: Just like everybody does who use the hotel network.

Leo: Right. At that point I'm not encrypted. I haven't turned on my VPN yet.

Steve: Correct.

Leo: So she would be vulnerable for that brief period if she had folders filesharing turned on; yes?

Steve: Oh, I think she said that she had them on her work machine.

Leo: So she's safe, okay.

Steve: Yeah, so she's safe. But you're right. While your traffic is not going through the VPN, you are not protected by the VPN.

Leo: So I get to the hotel. I log onto the hotel's network. And then I launch HotSpotVPN. I'm protected from now on. But there is that brief period of time when I'm not protected.

Steve: Right. The idea would be you would probably be using a personal firewall on your laptop if you're a telecommuter. That would provide you the protection. Then the VPN tunnel would pierce the firewall outbound, go to your work. That way, at no point are you at danger.

Leo: Got to turn on my firewall. A wireless TiVo user writes: Episode 13 convinced me to switch from WEP - which we've pointed out is broken...

Steve: Broke.

Leo: ...to WPA, which we pointed out works. It's the best way to protect a wireless network.

Steve: Yup.

Leo: Thank you, he says. My wife and I are using Macs, Tiger. So the switch was relatively painless. I did, however, have a follow-up question. Is there any way to continue using devices like the TiVo and others that, unfortunately, only support WEP? I'm willing to connect TiVo by wire; but I was curious, is there any bridging technology that won't compromise my network security?

Steve: The question's come up before, and I've thought about it a lot. The only solution that makes sense that I could recommend would be to get an older wireless access point and use two.

Leo: Bridge it into the network.

Steve: Exactly. You need to have a central access point, I mean, sorry, a central router on whatever connects you to the Internet. And then you'd have a WPA access point and a WEP access point. Basically you'd be running two wireless networks. One is secure, and one is not secure. And...

Leo: And it's only minorly not secure because you could still run WEP on that one...

Steve: You absolutely could run WEP on it if you wanted to. And the other advantage is...

Leo: Nobody's going to crack your TiVo data.

Steve: Exactly. The idea would be, you could just think of your unsecured wireless as, you know, anyone can have access to it. You might want to turn off the SSID broadcasting, and you could use Mac filtering. But the advantage then is, if people come over with a wireless laptop, they're able to use your unsecured network, and you're able to keep your WPA just to yourself.

Leo: Now, if I do that, so I allow them on my unsecured wireless network, the wireless access point getting into my secured network is preventing them access to my secured network; right? That's acting as a firewall between my friends, who I don't trust, apparently, and my network; right?

Steve: It turns out that something we have not covered yet, but we're going to very soon, as soon as we get back to our fundamental technology series, ARP spoofing is a real problem for LANs. And we'll be talking about why LANs are just not secure. So it turns out there's no safe way to have two wireless access points plugged into each other. They need to be plugged into a third router in a Y configuration. That's safe because ARP never crosses across routers. And so you get protection from spoofing. If you really want it to have the best security, you need a Y configuration.

Leo: We've mentioned that before, and we'll talk about ARP poisoning in greater detail later.

Steve: And this time I do have pictures.

Leo: Oh, good.

Steve: Yeah.

Leo: Too bad it's radio. Am I on John McFarland of Portland, Oregon?

Steve: Yeah.

Leo: He wonders: Regarding tunneling and VPNs, wouldn't using a tunnel for email, web surfing, peer-to-peer filesharing and so on, bypass any filtering, content management, port blocking, firewalling, and any other controls that a corporate or ISP bandwidth provider has set up to regulate the network's usage? For example, I'll give you an example that's very common. Some ISPs block BitTorrent.

Steve: Right.

Leo: So would using tunneling allow it?

Steve: Completely bypass all of that.

Leo: All right.

Steve: Yes. If your ISP doesn't allow this, or if your corporate network - I mean, now, I've got to say, last time we talked about this, all kinds of people...

Leo: People got mad.

Steve: ...got pissed off. And it's like, hey, we're not saying to do it. We're just talking about the technology.

Leo: We're warning you that it's possible, that your employees could be doing this.

Steve: Exactly. Tunneling technology means that the content in the tunnel is not filterable. It looks like - literally, it looks like noise. It's been encrypted. And anything correctly encrypted looks just like static. You can't tell the difference between it and random noise because they are random numbers.

Leo: And that's exactly why BitTorrent's proposing an encryption as part of the protocol, so that...

Steve: In order to prevent ISPs from snooping on their users.

Leo: Sniffing around.

Steve: Yeah.

Leo: Philip Hanson of Wilmington, Delaware, writes: Last week you talked about how DHCP servers provide IP addresses. But you also said they provide the computer's DNS server address. Uh-oh, what's a DNS server? Uh-oh.

Steve: Okay. We're going to keep this simple.

Leo: We only have a few minutes left.

Steve: We're going to keep this simple.

Leo: The crew is coming back.

Steve: I thought it was an interesting question because, I mean, a lot of people will know what a DNS server is. But I wanted to answer Philip's question...

Leo: Well, people know, I think kind of practically, kind of what it does. But I don't know if people really know what it does.

Steve: Well, and we're not going to do the whole deep hierarchy of the Domain Name Service. Basically, though, Philip, what this does is, it's the thing that converts the human-style, readable Internet addresses...

Leo: GRC.com.

Steve: GRC.com, Microsoft.com, Google.com, whatever, those are - actually each one of those is also represented by one of those Internet dotted quad, you know, like, for example, GRC.com, 4.79.142.200. If you put into your browser 4.79.200 - I'm sorry. See, I can't even remember it myself.

Leo: You don't need to. That's the beauty of it.

Steve: But I never forget GRC.com.

Leo: Right, that's the beauty of it.

Steve: Yep. So that's what DNS does.

Leo: That's what it is, is directory information.

Steve: Yeah.

Leo: You may not remember Steve's phone number; but you know his name, you call directory information, they match it up with a number. Ultimately, that's what the browser needs, though, to surf to that address.

Steve: Well, and your whole computer, for other purposes. So it does make sense that DHCP is giving it, not only its IP address and the various other networking parameters, but also a server that it can use to look up the IP addresses of all the other places you want to go on the 'Net.

Leo: Basically fills out that form for you that you'd have to do by hand if you didn't have DHCP. Craig in the U.K. asks: In your first "How the Internet Works" episode, you explained that packets might be lost, but never explained how or why that could happen. If most packets make it across the Internet, why is it that some don't?

Steve: Good question. If you've ever watched a dripping faucet, most of the drips go in the same place. But every so often you get this bizarre one that just kind of - somehow it lands on the other side of the sink. It's like, wait a minute, you know...

Leo: You must spend a lot of time watching dripping faucets.

Steve: It's chaos theory, actually. And the Internet is like that. The idea is that, even though over the whole Internet there's a whole bunch of averaging going out...

Leo: It's pretty predictable.

Steve: Yes, it's very predictable and generally works. You do have little, sort of like little tsunamis on routers where suddenly everything will pile up. A router doesn't have tons of buffering. Basically the packets are coming in, and it's sending them out as soon as it can. But since it's got a bunch of connections, if a bunch of packets came all into it from three inputs, and they all wanted to go to the one output, for example, out the same path, there just isn't a way that it's able to take and cram three times the data out one output. So what the router does is just - it shrugs, and it says, oh, well. It sends what it can, and it drops the others. And the chances are just sending it again will not cause that same brief collision of not having enough bandwidth for just that instant. So that's how packets get lost. It's just little bitty times when there just isn't enough bandwidth on specific linkages.

Leo: Next week Steve's going to explain where those socks go when you dry them and you only get one back. Finally, Burt Lasarge from Redford, Michigan asks: I was just wondering where you guys frequent the 'Net as your favorite sources of tech information.

Steve: Good question.

Leo: Do you, like, browse around on the 'Net and look for information?

Steve: You know, I don't. I put the...

Leo: You're very goal oriented.

Steve: Yes.

Leo: When you go on the 'Net, you know what you're looking for.

Steve: That's exactly - I am Mr. Google.

Leo: You're not a browser.

Steve: Google, I know - exactly. I know exactly what I want. I have my Google set to my homepage. I just come up with a phrase, and it's just amazing how quickly I can find what I want. So I'm not in a mode where I'm, like, looking for more stuff. I'm really looking for answers to the problems I've already got.

Leo: I do, because it's kind of my job, I do kind of surf quite a bit. And I use a newsreader. And in fact, I'll tell you what, I'll put my OPML file up, if you want to see what links I use. That's the easiest way to do it. You can import it into any news aggregator, and there are about 60 different pages I go to.

Steve: Wow.

Leo: Well, I don't see - that's why an aggregator's nice. You don't have to actually go to those individual pages. It just loads the headlines for you, and you can look and scan through them. But for security information, I think SecurityFocus.com is a very good...

Steve: It's a great place.

Leo: And it's certainly a site that, if you wanted to know more about security on an ongoing basis, it would be worth visiting. They have a number of newsletters you can subscribe to in a lot of different areas of security so that, if anything big does happen, you'll be alerted by push, you know, you don't even have to go that site.

Steve: Right.

Leo: There's the Bugtraq mailing list, also, is another good mailing list where security exploits are quickly revealed.

Steve: Yeah, it's funny, I mean, the way I work, I'll Google for what I want, then I'll see SecurityFocus or Bugtraq or one of the sites I know really well. It's like, oh, good, now I've got the page...

Leo: I can trust it, too.

Steve: Exactly. So you bring your knowledge of those sites to the result of the search in order to sort of winnow it down further.

Leo: There are lots of great sites out there. I'll tell you what. I will start a - for those of you who are donors to TWiT.tv, I will start a thread in our message boards. We have new private message boards. Have you joined those message boards, Steve?

Steve: Yeah, I am, I'm a member.

Leo: I'll put a thread in there...

Steve: I couldn't figure it out. It was too complicated.

Leo: He's a Usenet type. I will put a thread in there of where do you go, because we'd like to hear from you where you go to find out more information, not only about security, but about tech subjects in general. And I will also put the OPML up in the show notes on TWiT.tv.

We're out of time. They've turned the lights back on in the studio. The camera crew's back. Fortunately the Olympics hockey is keeping them busy, so we don't have to worry for a few minutes. But I think we'd better wrap this thing up.

Steve: We're done anyway.

Leo: We're done anyway. All the questions are done. Well done. Next week what are we going to cover?

Steve: Next week we're going to talk about LAN Insecurity. We talked about how LANs work. So next week is how IP and Ethernet are joined together by this Address Resolution Protocol, ARP. And unfortunately why, since security was never even a consideration back when this was designed, why it's so frighteningly insecure.

Leo: That'll be great. Next week.

Steve: So cool technology with a real security overtone.

Leo: That's the March 2nd Security Now!. We invite you, of course, to visit Steve's website, GRC.com/securitynow.htm. That's where you'll find the transcripts, the 16KB version for the bandwidth-impaired. And of course it's where you can read all the show notes, as well.

Steve is the author of the fabulous SpinRite disk maintenance and recovery utility. I wouldn't leave home without it. In fact, I have it in my suitcase. I literally don't leave home without it. And if you have a hard drive that you want to keep an eye on, or if you just, you know, have something you're losing, maybe some files that you want to recover, this is the way to do it.

Steve: Someone wrote an amazing letter to us a couple days ago. I love to see those. Someone who just desperately needed something, and they didn't know what to do, and they ran SpinRite, and just it's fun to hear them describe how they just - they can't believe, when they reboot their machine after running SpinRite, it's back.

Leo: Yeah, it's really neat. That's GRC.com for SpinRite, and of course the show notes. And we thank our friends at AOL Radio for broadcasting the show on their podcast channel and providing the bandwidth so that we can give you Security Now! every week: AOLmusic.com.

TWiT.tv is the headquarters for the entire TWiT network. If you like what you hear, please feel free to click those donation buttons. And of course everybody who donates, whether it's a dollar or a hundred, gets access to the TWiT Forums and other cool stuff, which we're still trying...

Steve: Working on.

Leo: Working on. We'll find something. We'll see you next week. Thank you, Steve. Have a safe trip home.

Steve: Always a pleasure. Good to see you in the flesh this time.

Leo: Yes, so to speak. I'll have to put my clothes back on, though, for the show. This is Security Now!.